National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Xerox® AltaLink™ C8030/C8035/C8045/C8055/C8070

Report Number: CCEVS-VR-VID10955-2019

Dated: July 22, 2019

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
National Security Agency
9800 Savage Road
Fort Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jerry Myers

Marybeth Panock

Harry Beddo

The Aerospace Corporation

Evaluation Team

Brian Pleffner

Cheryl Dugan

Eve Pierre

DXC Technology

Table of Contents

List of Tables

1. Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Xerox® AltaLink™ C8030/C8035/C8045/C8055/ C8070, the Target of Evaluation (TOE), performed by DXC Technology Security Testing and Certification Laboratory (STCL). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by DXC Technology (DXC) of Annapolis Junction, MD in accordance with the United States evaluation scheme and completed in July 2019. The information in this report is largely derived from the ST, and the evaluation sensitive documents: Evaluation Technical Report (ETR) and the functional testing report, which are summarized in the Assurance Activity Report. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated September 2012, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 4, September 2012.

The Xerox® AltaLink™ C8030/C8035/C8045/C8055/ C8070, is a multi-function device that copies and prints with scan and fax capabilities.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	Xerox® AltaLink™ C8030/C8035/C8045/C8055/ C8070 System Software version: 100.001/2/3.008.27400 with patch 347567v2.dlm
Sponsor and Developer	Xerox Corporation 800 Phillips Road Rochester, NY 14580
CCTL	DXC Technology 10830 Guilford Road, Suite 308 Annapolis Junction, Maryland 20701
Completion Date	July 19, 2019

Item	Identifier
Interpretations	There are the following Technical Decisions for this evaluation. 0393 – Require FTP_TRP.1(b) only for printing 0299 – Update to FCS_CKM.4 Assurance Activities 0261 – Destruction of CSPs in flash 0253 – Assurance Activities for Key Transport 0219 – NIAP Endorsement of Errata for HCD PP v1.0 0176 – FDP_DSK_EXT.1.2 - SED Testing 0157 – FCS_IPSEC_EXT.1.1 - Testing SPDs 0074 – FCS_CKM.1(a) Requirement in HCD PP v1.0
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 5, April 2017
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Protection Profile	Protection Profile for Hardcopy Devices, Version 1.0, 10 September 2015 and Errata for the Hard Copy Device Protection Profile v1.0.
Disclaimer	This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.
Evaluation Personnel	Brian Pleffner Cheryl Dugan Eve Pierre DXC Technology
Validation Personnel	Jerry Myers Marybeth Panock Harry Beddo The Aerospace Corporation

2. Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Product Compliant List (PCL).

Table 2 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated
- The Security Target (ST), describing the security features, claims, and assurances of the product

Table 2: Evaluation Identifiers

Item	Identifier
ST Title and Version	Xerox® AltaLink™ C8030/C8035/C8045/C8055/ C8070 Security Target version 0.6
Publication Date	July 22, 2019
Vendor	Xerox Corporation
ST Author	DXC Technology; Eric Jacksch
Target of Evaluation Reference	Xerox® AltaLink™ C8030/C8035/C8045/C8055/ C8070
TOE Software Version	100.001/2/3.008.27400 with patch 347567v2.dlm
Keyword	Multi-function Device

3. Security Policy

The core functionality of the Xerox® AltaLink™ C8030/C8035/C8045/C8055/ C8070 is the ability to define and enforce security policies to the protect the data transmitted to the multifunction device.

4. Security Problem Definition

4.1. Assumptions

The ST identified the following security assumptions contained in Table 3:

Table 3: Secure Usage Assumptions

ID	Assumptions
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

4.2. Threats

The ST identified the following threats addressed by the TOE:

Table 3: Threats Addressed

ID	Threats
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE.

T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

4.3. Organizational Security Policies

The Security Target identifies the following Organizational Security Policies (OSPs) to which the TOE must comply.

Table 4: Organizational Security Policies

ID	Organizational Security Policy
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION (conditionally mandatory)	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL (conditionally mandatory)	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.
P.FAX_FLOW (conditionally mandatory)	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.
P.IMAGE_OVERWRITE (optional)	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices.
P.PURGE_DATA (optional)	The TOE shall provide a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices.

5. Architectural Information

5.1. Physical Scope and Boundary

The TOE is an MFD (Xerox® AltaLink™ C8030/C8035/C8045/C8055/ C8070) that consists of a printer, copier, scanner, fax and associated administrator and user guidance. The TOE comprises all software and firmware within the MFD enclosure.

Users can determine version numbers and whether the Xerox Embedded Fax Accessory, Xerox Workflow Scan Accessory and Image Overwrite Security Package are installed by reviewing the TOE configuration report.

5.2. Required Non-TOE Hardware, Software, and Firmware

The TOE does not require any additional hardware, software or firmware in order to function as a multi-function hard copy device. Additional features require non-TOE support as follows:

- Network security and fax flow features are only useful in environments where the TOE is connected to a network or PSTN.
- Network identification is only available when LDAP remote authentication services are present in the environment.
- Smart card authentication requires Federal Information Processing Standard (FIPS) 201 Personal Identity Verification Common Access Card (PIV-CAC) compliant smart cards and readers or equivalent. In support of smart card authentication, a Windows Domain Controller must also be present in the environment.
- The TOE may be configured to reference an NTP server for time.

6. Logical Scope of the TOE

The TOE provides the following security features:

Identification and Authentication

In the evaluated configuration, the TOE requires users and system administrators to authenticate before granting access to user (copy, print, fax, etc.) or system administration functions via the Web User Interface (Web UI) or the Local User Interface (LUI). The user or system administrator must enter a username and password at either the Web UI or the LUI. The password is obscured as it is being entered. The TOE provides role based access control as configured by the system administrator.

The TOE also supports smart card and Lightweight Directory Access Protocol (LDAP) for network authentication.

Security Audit

The TOE generates audit logs that track events/actions (e.g., print/scan/fax job submission) to identified users. The audit logs, which are stored locally in a 15000-entry circular log, are available to TOE administrators and can be exported in comma separated format for viewing and analysis.

Access Control

The TOE enforces a system administrator defined role-based access control policy. Only authenticated users assigned to roles with the necessary privileges are allowed to perform copy, print, scan or fax on the TOE via the Web UI or the LUI.

Unauthenticated users can submit print or LanFax jobs to the TOE via printing protocols. Release of unauthenticated print jobs to the hardcopy output handler is dependent on the system administrator defined policy.

The TOE allows filtering rules to be specified for IPv4 network connections based on IP address and port number.

Security Management

A Local User, via the local user interface, or a Remote User, via the browser-based interface, with administrative privileges can configure the security settings of the TOE. The TOE has the capability to assign Users to roles that distinguish Users who can perform administrative functions from Users who can perform User functions via a role based access control policy. The TOE also has the capability to protect its security settings from unauthorized disclosure and alteration when they are stored in the TOE and in transit to or from the browser-based interface.

Trusted Operation

The TOE includes a software image verification feature and Embedded Device Security which employs McAfee software to detect and prevent unauthorized execution and modification of TOE software.

Encryption

The TOE utilizes digital signature generation and verification (RSA), data encryption (AES), key establishment (RSA) and cryptographic checksum generation and secure hash computation (HMAC, SHA-1) in support of disk encryption, SSH, TLS, TLS/HTTPS, TLS/SMTP and IPsec. The TOE also provides random bit generation in support of cryptographic operations.

The TOE stores temporary image data created during a copy, print, scan and fax job on the single shared hard disk drive (HDD) that is field replaceable. This temporary image data consists of the original data submitted and additional files created during a job. All partitions of the HDD used for spooling temporary files are encrypted. The hard drive encryption key is derived from a BIOS saved passphrase and is the same value after each power-up (see KMD for details).

Trusted Communication

The TOE provides support for a number of secure communication protocols:

- Transport Layer Security (TLS) support is available for protecting communication over the Web User Interface (Web UI) and SMTP email communications.
- Secure Shell (SSH) File Transfer Protocol (SFTP) and TLS are available for protecting document transfers to a remote file depository.
- Internet Protocol Security (IPsec) support is available for protecting communication over IPv4 networks.
- TLS support is available for protecting communication with a remote authentication server.

PSTN Fax-Network Separation

The TOE provides separation between the fax processing board and the network interface and therefore prevents an interconnection between the PSTN and the internal network. This separation is realized in software, as by design, these interfaces may only communicate via an intermediary.

Data Clearing and Purging

The image overwrite feature overwrites temporary image files created during a copy, print, scan or fax job when those files are no longer needed. Overwrite is also invoked at the instruction of a job owner or administrator and at start-up. The purge feature allows an authorized administrator to permanently delete all customer-supplied data on the TOE. This addresses residual data concerns when the TOE is decommissioned from service or redeployed to a different environment.

7. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *Xerox AltaLink C80XX Series Multifunction Printer User Guide, Version 2.0*
- *Xerox AltaLink Series Multifunction Printer System Administrator Guide, Version 2.0*
- *Secure Installation and Operation of Your AltaLink B8045 / B8055 / B8065 /B8075 / B8090 Multifunction Printer and AltaLink C8030 / C8035 / C8045 / C8055 / C8070 Color Multifunction Printer Version 1.6*

The above products are the only documents delivered with the product. If any additional document is received with the TOE it was not covered by the scope of this evaluation and

should not be trusted to configure, administer, or use the TOE in its evaluated configuration.

8. Evaluated Configuration

The evaluated configuration consist the Xerox MFP – AltaLink Models C8030, C8035, C8045, C8055, and C8070 when configured in accordance with the guidance provided in the documents listed in Section 7.

9. IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information provided in the Assurance Activity Report, which provides a non-proprietary overview of the testing that is documented in the proprietary Evaluation Technical Report.

9.1. Evaluation team independent testing

The evaluation team conducted independent testing at the Xerox Corporation in Rochester, NY. The evaluation team maintained complete control over the test network and evaluated configuration in accordance with the laboratories policies and procedures for performing testing at a vendor facility. The evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Assurance Activities.

Each Assurance Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

9.2. Test Configuration and Test Tools

A summary of the test configurations and the test tools that were used during the evaluation may be found in Section 7 of the Assurance Activity Report.

The test configuration used the Xerox MFP – AltaLink™ C8045.

The TOE is connected to a hub, which, two Windows 10 machines, an Ubuntu machine, and a Windows 2012 server machine is also connected.

The Windows 2012 Server functions as a Domain Controller, DNS Server, and File Server and hosts an IIS server.

Use the Secure Installation and Operation User Guide to Set-up TOE in the Evaluated Configuration.

Set up and configure TOE by using the following security protocols and functions in the evaluated configuration by following the guidelines below to:

1. In General Set Up, print out a configuration report. Verify software version is the same as the version in the ST.
2. In General Set up verify the time and date of TOE are correct. If not correct, then change so date and time are current.

3. Very that the Immediate Image Overwrite is enabled. If not enabled, select enable.
4. Very that the On- Demand Image Overwrite is enabled. If not enabled, select enable.
5. Very that Data Encryption is enabled. If it is not, select enable
6. Very that FIPS 140-2 Mode is enabled. If not enabled, perform the following steps;
   i. Select the enabled button.
   ii. Select the Run Configuration Check and Apply button.
   iii. Select Change to 2048-bit button.
   iv. In the next screen select the 2048 bit.
   v. Select the Manage and Delete Certificates.
   vi. Select 'Root/Intermediate Trusted Certificate(s)' tab.
   vii. View and select the certificates that do **not** comply with the minimum key length value of 2048. Now Click 'Delete Selected' button. Followed by [OK] button to delete the selected certificates.
   viii. Again, go to [Security] followed by [Encryption] → [FIPS 140-2]. Select the [Enable] option and click [Run Configuration Check & Apply] button.
   ix. Check the 'Enable non-FIPS 140-2 exception' option and click 'Acknowledge Kerberos Exception' button.
   x. Select [Reboot Machine] button followed by [OK] button.
7. Verify that IP Filtering is enabled and IP Filtering (defaults to no rules defined).
8. Verify that Audit Log is enabled. If not enabled, select enable.
9. Enable HTTPS by performing the following steps;
   i. From the properties menu, navigate to [Connectivity] → [Setup] → [HTTP].
   ii. Select the 'No (Requests can be made over HTTP and HTTPS)' option button under 'Force Traffic over SSL' and then Click [Save].
   iii. Select the 'Yes (All HTTP requests will be switched to HTTPS)' option button under 'Force Traffic Over Secure Connection (HTTPS)' and ensure the port number text box is set to 443, then click [Save].
   iv. Log back into the TOE using HTTPS.
   v. Select the 'Yes (All HTTP requests will be switched to HTTPS)' option button under 'Force Traffic over Secure Connection (HTTPS)' and ensure the port number text box is set to 443, then click [Save].
10. Ensure that TLS 1.1 is used on TOE by performing the following steps:

i. In Properties select Security>Encryption>TLS Encryption.

ii. Select TLS.1.1 and above.

iii. Apply to Save change.

11. Install a digital certificate on device by performing the following steps:

i. Click certificates and select Security Certificates.

ii. Select the Xerox Device Certificate tab

iii. Create a New Xerox Device Certificate

iv. Complete the requested form

v. Click Finish (may have to re logon and add exception)

12. Verify that IPsec is enabled. If not enabled, select enable.

13. Set Password Requirements. In Login/Permissions/Accounting go to Device User Database and perform the following password requirement steps:

i. Select Password Settings tab

ii. Specify minimum of 8 characters and maximum length of 15

iii. Check Cannot contain Friendly Name, Contain User Name and Must contain at least one number.

14. Set logon method. In Login/Permissions/Accounting go to Login Methods. Ensure that Control Panel and Website Login methods are set to 'Validate on the Network'.

15. Create a User. In Login/Permissions/Accounting go to Device User Database and perform the following Add New User steps:

i. Create a user name and friendly name

ii. Create password and retype password

iii. Save

16. Create User Permissions. In Login/Permissions/Accounting go to Device User Database and Select permissions on user created and ensure Tools and Apps are locked.

17. Ensure Session Inactivity Timeout is configured. In Security select Timeout & Resume. For the User Interface System Timeout enter 6 minutes. For the Web User Interface System Timeout enter 7 minutes.

18. TOE uses the primary LDAP server for authentication. No configuration is needed.

19. USB Port Security. (Both the front and rear USB Ports are enabled by default). Ports can be disabled by unchecking boxes.

20. SFTP Filing (only for transfer of the audit log to an audit log server). Ensure SFTP Filing (defaulted to passive mode).

21. Change admin password from 1111 to a secure password.

9.3. Vulnerability Analysis

The evaluation team performed a vulnerability analysis of the TOE evidence and a search of publicly available information to identify potential vulnerabilities in the TOE. An overview of the vulnerability analysis that includes a complete list of the search terms used, the databases searched, and the date when those searches were performed may be found in Section 6.7 of the Assurance Activity Report. Based on the results of this effort, there were no identifiable vulnerabilities found at the time of certification.

10. Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1R4. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R4.

DXC Technology has determined that the product meets the security criteria in the Security Target, which specifies conformance to the Protection Profile for Hardcopy Devices, Version 1.0, 10 September 2015. A team of validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on July 19, 2019.

11. Validator Comments

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the devices, to include software, firmware, or hardware that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

Of particular note, there are authentication methods described in the System Administrator's Guide and the User's Guide that are not supported in the evaluated configuration. In the evaluated configuration only smart cards and LDAP are supported.

Also, significantly, personal USB storage devices are not supported in the evaluated configuration. The vendor has specified that if an USB port needs to be used to perform a function like diagnostics or installing a software upgrade, the applicable host or target USB port should be temporarily enabled while the applicable function is being performed, and then when the function is competed it should be immediately disabled again.

All other items and scope issues have been sufficiently addressed elsewhere in the document.

12. Annexes

None

13. Security Target

Xerox Multi-Function Device Xerox® AltaLink™ C8030/C8035/C8045/C8055/ C8070 Security Target, Version 0.6.

GLOSSARY

- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
CSC	DXC Technology
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFD	Multi-Function Device
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

15. Bibliography

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012.
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 5, April 2017.
5. Protection Profile for Hardcopy Devices, Version 1.0, September 10, 2015, with Errata #1 June 2017
6. Xerox Multi-Function Device Xerox® AltaLink™ C8030/C8035/C8045/C8055/C8070 Security Target, Version 0.6, July 2019
7. Secure Installation and Operation of Your AltaLink™ C8030/C8035/C8045/C8055/ C8070 Multifunction Printer AltaLink™ C8030/C8035/C8045/C8055/C8070 Multifunction Printer, Version 1.7, July 17, 2019
8. Xerox® AltaLink Series® Multifunction Printer System Administrator Guide, Version 2.0, October 2018
9. Xerox® AltaLink™ C80XX Multifunction Printer User Guide, 2.0, October 2018
10. Xerox Key Management Description for Xerox Atlantis Multi-Function Device, Version 1.5, March 28, 2018
11. Xerox C8030/C8035/C8045/C8055/ C8070 Entropy Assessment Report, Version 1.0, May 2019
12. Xerox Evaluation Technical Report for Xerox AltaLink™ C8030 / C8035 / C8045 / C8055 / C8070 Document version: 1.3, July 2019
13. Assurance Activity Report: Xerox® AltaLink™ C8030/C8035/C8045/C8055/C8070 Document version: 1.3, July 2019
14. Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8070, Detailed Test Report, v1.2, July 2019